



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,808	12/26/2000	Masayuki Terao	Q62445	2609

7590 05/25/2004
SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 05/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/745,808

Applicant(s)

TERAO ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 17 October 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Priority

1. The foreign priority has been made in this application.
2. The effective filing date for the subject matter defined in the pending claims in this application is 12/27/1999 on the benefit of foreign priority date.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1 – 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Shigeki (Publication Number: 729694), hereinafter referred to as Shigeki.
2. As per claim 1, Tamiyuki teaches a communication device which can be freely inserted into and extracted from a slot of a terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101).

Art Unit: 2131

3. Tamiyuki does not teach said communication device exposed from said terminal device when inserted into said slot is applied a color according to a kind of the communication device.

4. Shigeki teaches said communication device exposed from said terminal device when inserted into said slot is applied a color according to a kind of the communication device (Shigeki: see for example, Paragraph [0009] and Figure 1).

5. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shigeki within the system of Tamiyuki because the visibility is improved by coloring the terminator case in accordance with the terminator type, and marking the color of said case visible from outside even when it is inserted into a connector inside a base opening.

6. As per claim 2, Tamiyuki-Shigeki teaches the claimed invention as described above (see claim 1). Tamiyuki further teaches communication device comprising a radio unit adapted to a predetermined mobile communication service (Tamiyuki: see for example, Paragraph [0017] and Figure 1 Element 101).

7. Tamiyuki does not teach applying a color according to a kind of the mobile communication service.

8. Shigeki teaches applying a color according to a kind of the mobile communication service (Shigeki: see for example, Paragraph [0009] and Figure 1).

9. Same rational for combination applies here as above in rejecting claim 1.

10. As per claim 3, Tamiyuki-Shigeki teaches the claimed invention as described above (see claim 1). Tamiyuki further teaches mobile communication service in which

Art Unit: 2131

part information necessary for the connection to a specific provider is stored (Tamiyuki: see for example, Paragraph [0015]. Tamiyuki discloses the device comprises information necessary for connecting to the line).

11. As per claim 4, Tamiyuki-Shigeki teaches the claimed invention as described above (see claim 1). Tamiyuki further teaches communication device being a communication device to wireless-connect terminal devices (Tamiyuki: see for example, Paragraph [0017] and Figure 1 Element 101). Tamiyuki does not teach applied said color according a transmission rate.

12. Shigeki teaches applied said color according a transmission rate (Shigeki: see for example, Paragraph [0009] and Figure 1: Shigeki teaches coloring the terminator case in accordance with the terminator type. The terminator type is well known defined by its transmission rate as one of the crucial operating parameters).

13. Same rational for combination applies here as above in rejecting claim 1.

14. As per claim 5, Tamiyuki teaches a set of a plurality of communication devices which can be freely inserted into and extracted from a slot of a terminal device and have radio units adapted to different mobile communication services (Tamiyuki: see for example, Paragraph [0008], Paragraph [0017] and Figure 1 Element 101).

15. Tamiyuki does not teach a part of said communication device exposed from said terminal device when inserted into said slot is applied a different color for each communication device.

Art Unit: 2131

16. Shigeki teaches a part of said communication device exposed from said terminal device when inserted into said slot is applied a different color for each communication device (Shigeki: see for example, Paragraph [0009] and Figure 1).

17. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shigeki within the system of Tamiyuki because the visibility is improved by coloring the terminator case in accordance with the terminator type, and marking the color of said case visible from outside even when it is inserted into a connector inside a base opening.

18. Claims 6, 16 – 21 and 23 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu.

19. As per claim 6, Tamiyuki teaches a communication device which can be freely inserted into and extracted from a slot of a terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101).

20. Tamiyuki does not teach a method of conducting authentication between a communication device and said terminal device.

21. Vu teaches a method of conducting authentication between a communication device which can be freely inserted into and extracted from a slot of a terminal device and said terminal device, comprising the steps of:

Art Unit: 2131

a. inserting a key module storing the same ID as an ID stored in the communication device into the slot to register the ID stored in the key module at the terminal device (Vu: see for example, Column 4 Line 42 – 62 and Column 2 Line 62 – 65: Vu discloses “two factors authentication” using not only the cryptographic information but also the PIN (i.e. Identification Number ID) to reduce the risk of a security breach (Vu: see for example, Column 4 Line 44 – 45). Vu also discloses that the information (such as ID and cryptographic information) for registration and validation purpose can be initially stored on a BIOS ROM or copied from a removable storage device, such as a floppy disk or dongle (Vu: see for example, Column 4 Line 57 – 60 and Column 4 Line 62 – 64). The key module in the claim limitation herein is indeed qualified as a dongle (as a removable storage) to store the ID for registration and later validations.

b. Vu teaches conducting collation between the terminal device and the communication device inserted into the slot to determine whether the ID stored in the communication device and the ID registered at the terminal device coincide with each other (Vu: see for example, Column 4 Line 51: Vu discloses the token to be inserted into the slot (as equivalent to the communication device from authentication perspective) contains the same ID as the ID registered initially (Vu: see for example, Column 4 Line 52).

22. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively established.

Art Unit: 2131

23. As per claim 16, Tamiyuki teaches a plurality of communication devices which can be freely inserted into and extracted from a slot of a terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101). Tamiyuki does not teach each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device and a common key for data encryption inherent to the set.

24. Vu further teaches each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device (see same rationale in rejecting part of the claim 12) and a common key for data encryption inherent to the set (see same rationale in rejecting the claim 13).

25. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively established and the unique ID also resolves part of the communication addressing issue within a group of wireless devices.

26. As per claim 18, Tamiyuki teaches a plurality of communication devices which can be freely inserted into and extracted from a slot of a terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101). Tamiyuki does not teach each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device, a public key for data encryption and a secret key for data decoding.

27. Vu teaches each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device

Art Unit: 2131

(see same rationale in rejecting part of the claim 12), a public key for data encryption and a secret key for data decoding (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a private key in the public key cryptography system. However, a person of ordinary skill in the art at the time the invention was made would realize that the device only uses the private key of own device for data decoding and the public key for data encryption), which is inherited from the asymmetric cryptographic systems.

28. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively established and the unique ID also resolves part of the communication addressing issue within a group of wireless devices.

29. As per claim 17 and 19, Tamiyuki-Vu teaches the claimed invention as described above (see claim 16 and 18 respectively). Vu further teaches a part of the communication device partly projecting from the terminal device when inserted into the slot of the terminal device is assigned a number inherent to the communication device (see the same rationale in rejecting the claim 12: The unique ID for authentication purpose is a number as well as an unique address).

30. Tamiyuki as modified does not teach the communication address of the communication device is composed of a high-order address part and a low-order address part in which part said number is set

31. However, a person of ordinary skill in the art at the time the invention was made would realize that the IP subnet address composes two parts where the high-order

Art Unit: 2131

address part corresponds to the network address and the low-order address part corresponds to the specific Host ID.

32. Same rational for combination applies here as above in rejecting claim 16.

33. As per claim 20, Tamiyuki teaches a method of locally wireless-connecting a plurality of terminal devices by using a set of a plurality of communication devices which can be freely inserted into and extracted from a slot of the terminal device to wireless-connect the terminal devices and which have a memory for storing a communication address of the own communication device, comprising the steps of:

a. allocating a communication device to each of the terminal devices to be wireless-connected (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101).

Tamiyuki does not teach inserting each communication device into a slot of other terminal device than the allocated terminal device to register a communication address stored in the memory of the communication device at a transmission destination list table of the terminal device into which the communication device is inserted.

34. Vu teaches:

35. b. inserting each communication device into a slot of other terminal device than the allocated terminal device to register a communication address stored in the memory of the communication device at a transmission destination list table of the terminal device into which the communication device is inserted (Vu: see for example, Column 4 Line 57 – 60 and Column 4 Line 62 – 64: Vu discloses that the information (such as ID and cryptographic information) during the system setup can be initially

Art Unit: 2131

stored on a BIOS ROM or copied from a removable storage device (a token in general), such as a floppy disk or dongle (Vu: see for example, Column 4 Line 57 – 60 and Column 4 Line 62 – 64). The communication device module in the claim limitation herein is indeed qualified as a token (as a removable storage) to store the ID during system setup,

36. Furthermore, a group of unique IDs can be served as a group of unique addresses, in general, to facilitate the communication within a group of devices. Therefore, each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device and a communication address of other communication device of the same set.

37. Vu does not expressly teach sequentially inserting communication devices allocated to other terminal devices to register communication addresses so that a communication address of other communication device of the same is also stored inside a memory readable by said terminal device.

38. However, It would have been obvious to a person of ordinary skill in the art at the time the invention was made to setup the addresses within a group of wireless devices by sequentially inserting communication devices allocated to other terminal devices to register communication addresses because the destination address must be known to the transmission source and manual configuration from the keypad or automatic download from another node are not available as the design options according to the claim limitation,

Art Unit: 2131

39. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively established and the unique ID also resolves part of the communication addressing issue within a group of wireless devices,

c. inserting each communication device into a slot of an allocated terminal device, and by using communication addresses of a transmission destination communication device and a transmission source communication device as a transmission destination address and a transmission source address, transmitting and receiving data between the terminal devices into which the communication devices are inserted. However, a person of ordinary skill in the art at the time the invention was made would realize the source and destination addresses are the mandatory header fields in the communication protocol.

40. As per claim 21, Tamiyuki-Vu teaches the claimed invention as described above (see claim 20). Vu further teaches said memory of each communication device, a common key inherent to the set is stored, said common key being for use in encryption of transmission data and decoding of reception data (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a common key in the symmetric key system).

41. Same rational for combination applies here as above in rejecting claim 20.

42. As per claim 25, Tamiyuki teaches a method of locally wireless-connecting a plurality of terminal devices by using a set of a plurality of communication devices which

Art Unit: 2131

can be freely inserted into and extracted from a slot of the terminal device to wireless-connect the terminal devices and which have a memory for storing a communication address, a public key and a secret key of the own communication device, comprising the steps of:

a. allocating a communication device to each of the terminal devices to be wireless-connected (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101).

Tamiyuki does not teach inserting each communication device into a slot of other terminal device than the allocated terminal device to register a communication address stored in the memory of the communication device at a transmission destination list table of the terminal device into which the communication device is inserted.

43. Vu teaches:

b. inserting each communication device into a slot of other terminal device than the allocated terminal device to register a communication address and a public key stored in the communication device at a transmission destination list table of the terminal device into which the communication device is inserted (Vu: see for example, Column 4 Line 57 – 60 and Column 4 Line 62 – 64: see same rationale in rejecting the claim 20(b) and the claim 14).

c. inserting each communication device into a slot of an allocated terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101, and

d. by using communication addresses of a transmission destination communication device and a transmission source communication device as a transmission destination address and a transmission source address, using a public key of the transmission

Art Unit: 2131

destination communication device for the encryption of transmission data and using a secret key for the decoding of reception data, transmitting and receiving data between the terminal devices into which the communication devices are inserted.

44. Vu further teaches said memory of each communication device, a secret key of the own communication device and a public key of other communication device of the same set are stored (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a private key in the public key cryptography system. However, a person of ordinary skill in the art at the time the invention was made would realize that the device only uses the public keys of other devices (not the private keys) to encrypt and transmit the data to the destination (i.e., other devices), which is inherited from the asymmetric cryptographic systems.

45. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively,

46. As per claims 23/24 and 26/27, Tamiyuki-Vu teaches the claimed invention as described above (see claims 20, 25 respectively). Vu further teaches a part of the communication device partly projecting from the terminal device when inserted into the slot of the terminal device is assigned a number inherent to the communication device (see the same rationale in rejecting the claim 12: The unique ID for authentication purpose is a number as well as an unique address).

Art Unit: 2131

47. Tamiyuki as modified does not teach the communication address of the communication device is composed of a high-order address part and a low-order address part in which part said number is set

48. However, a person of ordinary skill in the art at the time the invention was made would realize that the IP subnet address composes two parts where the high-order address part corresponds to the network address and the low-order address part corresponds to the specific Host ID.

49. Same rational for combination applies here as above in rejecting the claim 20 and 25.

50. Claims 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu, and in view of de la Huerga (Patent Number: 5960085), hereinafter referred to as de la Huerga.

51. As per claim 7, Tamiyuki-Vu teaches the claimed invention as described above (see claim 6). Tamiyuki as modified does not teach when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted.

Art Unit: 2131

52. de la Huerga teaches when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted (de la Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 1 – 11: de la Huerga teaches a security system equipped with a wireless device to exchange authentication information with the security badge of a system user (de la Huerga: see for example, Column 4 Line 42 – 43). After the authentication and system in service, the computer terminal continues to monitor the signal path between the security badge and the computer terminal. If the system user turns away from the computer terminal, then the keyboard is locked and the screen is blanked off (de la Huerga: see for example, Column 5 Line 3 – 5).

53. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of de la Huerga within the system of Tamiyuki-Vu because de la Huerga teaches a limited access system for restricting and monitoring between smart devices.

54. As per claim 8, Tamiyuki-Vu teaches the claimed invention as described above (see claim 6). Tamiyuki as modified does not teach when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted.

55. de la Huerga teaches when the communication device is extracted from the slot after authentication between the terminal device and the communication device is

Art Unit: 2131

obtained, bringing the terminal device to a locked state where none of input by a user is accepted (de la Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 1 – 11).

56. Tamiyuki as modified does not teach when the communication device is inserted into the slot of the locked terminal device to obtain authentication between the terminal device and the communication device, releasing the terminal device from the locked state.

57. de la Huerga teaches when the communication device is inserted into the slot of the locked terminal device to obtain authentication between the terminal device and the communication device, releasing the terminal device from the locked state (de la Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 10 – 11: de la Huerga teaches if the security badge is not properly positioned for more than a preset period of time, the system user will be logged off automatically. This implies the system user needs to go through the authentication process again after returning back to the proper position).

58. Same rational for combination applies here as above in rejecting the claim 7.

Art Unit: 2131

59. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu, and in view of Billstrom (Patent Number: 5729537), hereinafter referred to as Billstrom.

60. As per claim 9, Tamiyuki teaches a communication device which can be freely inserted into and extracted from a slot of a terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101). Tamiyuki does not teach a method of conducting authentication between a communication device and said terminal device.

61. Vu teaches a method of conducting authentication between a communication device which can be freely inserted into and extracted from a slot of a terminal device and said terminal device, comprising the steps of:

- a. inserting a key module storing the same ID and authentication code as an ID and an authentication code stored in the communication device and storing a cryptographic function paired with an inverse cryptographic function stored in the communication device into the slot to register the ID, the authentication code and the cryptographic function stored in the key module at the terminal device (Vu: see for example, Column 4 Line 57 – 60), and
- b. when the communication device is inserted into the slot, conducting authentication between the communication device and the terminal device, said step (b) including:

Art Unit: 2131

(b-1) collating the ID stored in the communication device and the ID registered at the terminal device (Vu: see for example, Column 4 Line 51),

(b-2) when collation of IDs succeeds, generating a random number, sending data obtained by encrypting the random number with the authentication code connected by the cryptographic function from the terminal device to the communication device and at the communication device side, restoring the authentication code and the random number by the inverse cryptographic function to collate the restored authentication code and the stored authentication code (Vu: see for example, Column 4 Line 43 – 45, Column 6 Line 66 – 67, and Column 7 Line 1 – 2: Vu teaches decrypting after encrypting the authentication code, i.e. the KEYid herein. The authentication code is further processed using a hash function to compare the hashed digest. The claim limitation herein only compares the raw authentication code after decryption without further applying the hash function. It would have been an obvious matter of design choice to accommodate this difference because either way would be just as efficient.

62. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively established and the unique ID also resolves part of the communication addressing issue within a group of wireless devices.

63. Furthermore, when collation of authentication codes succeeds, Vu discloses one entity sends a random number to the other entity as a challenge (Vu: see for example, Column 1 Line 40 – 41);

Art Unit: 2131

64. Vu does not specifically teach how to manage the random number for authentication purpose. Billstrom teaches:

(b-3) sending data obtained by encrypting said restored random number by the inverse cryptographic function from the communication device to the terminal device and at the terminal device, restoring the random number by the cryptographic function to collate the restored random number with said random number generated by the own terminal device (Billstrom: see for example, Column 12 Line 53 – 60: Billstrom discloses GSM security using random number RAND for authentication. The source entity sending the random number RAND to the destination entity that generates the signed response SRES by encrypting the received random number RAND and returns SRES back to the source entity. The source entity compares the received signed response SRES with the result by encrypting the original random number RAND. It would have been an obvious matter of design choice to accommodate this difference because either way would just work equally as well from authentication viewpoints. In fact, the GSM mechanism requires only two times of cryptographic processing (both are encrypting) while the claim limitation herein takes 2 – 4 times of cryptographic processing (two encrypting and two decrypting) depends on the first comparison result of authentication code).

65. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Billstrom within the system of Tamiyuki-Vu because Billstrom teaches the GSM random number manipulating mechanism in light of the disclosure of using random number for authentication as taught by Vu.

Art Unit: 2131

66. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu, and in view of Koenck (Patent Number: 6006100), hereinafter referred to as Koenck,

67. As per claim 22, Tamiyuki-Vu teaches the claimed invention as described above (see claim 20). Tamiyuki as modified does not teach into one slot of a relay device having a plurality of slots and having a function of relaying data between slots, a communication device of a first set is inserted and into other one slot, a communication device of a second set is inserted to enable communication between a terminal device into which other communication device of the first set is inserted and a terminal device into which other communication device of the second set is inserted through said relay device.

68. Koenck teaches a relay device uses dual transceivers to relay data messages between two different networks or group of devices (Koenck: see for example, Column 4 Line 53 – 57).

69. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Koenck within the system of Tamiyuki-Vu because Koenck discloses a structure to relay two disjoint communication groups of devices in the physical layer.

Art Unit: 2131

70. Claims 12 – 15 and 28 – 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu, and in view of Aikawa (Patent Number: 5884047), hereinafter referred to as Aikawa,

71. As per claim 12, Tamiyuki teaches a plurality of communication devices which can be freely inserted into and extracted from a slot of a terminal device (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101). Tamiyuki does not teach each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device and a communication address of other communication device of the same set.

72. Vu teaches each communication device includes a memory readable by said terminal device and storing a communication address of the own communication device and a communication address of other communication device of the same set (Vu: see for example, Column 4 Line 57 – 60 and Column 4 Line 62 – 64: Vu discloses that the information (such as ID and cryptographic information) during the system setup can be initially stored on a BIOS ROM or copied from a removable storage device (a token in general), such as a floppy disk or dongle (Vu: see for example, Column 4 Line 57 – 60 and Column 4 Line 62 – 64). The communication device module in the claim limitation herein is indeed qualified as a token (as a removable storage) to store the ID readable by the terminal device during the system setup and an unique ID can be qualified as an unique communication address as well within a group of communication nodes.

Art Unit: 2131

73. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vu within the system of Tamiyuki because the security mechanisms can be effectively established and part of the address issues can also be resolved.

74. Tamiyuki as modified does not teach each communication device includes a memory readable by said terminal device and storing a communication address of other communication device of the same set.

75. Aikawa teaches each communication device includes a memory readable by said terminal device and storing a communication address of other communication device of the same set (Aikawa: see for example, Column 1 Line 53 – 57).

76. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Aikawa within the system of Tamiyuki-Vu because Aikawa teaches the address information of a static routing table for adjacent nodes can be stored inside a communication node of a network.

77. As per claim 13, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 12). Vu further teaches a common key for data encryption is stored in said memory of each communication device (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a common key in the symmetric key system).

78. Same rational for combination applies here as above in rejecting the claim 12.

79. As per claim 14, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 12). Vu further teaches said memory of each communication device,

Art Unit: 2131

a secret key of the own communication device and a public key of other communication device of the same set are stored (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a private key in the cryptography system. However, a person of ordinary skill in the art at the time the invention was made would realize that the device only uses the public keys of other devices (not the private keys) to encrypt and transmit the data to the destination (i.e., other devices), which is inherited from the asymmetric cryptographic systems.

80. Same rational for combination applies here as above in rejecting the claim 12.

81. As per claim 15, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 12). Vu further teaches a part of the communication device partly projecting from the terminal device when inserted into the slot of the terminal device is assigned a number inherent to the communication device (see the same rationale in rejecting the claim 12: The unique ID for authentication purpose is a number as well as an unique address).

82. Tamiyuki as modified does not teach the communication address of the communication device is composed of a high-order address part and a low-order address part in which part said number is set

83. However, a person of ordinary skill in the art at the time the invention was made would realize that the IP subnet address composes two parts where the high-order address part corresponds to the network address and the low-order address part corresponds to the specific Host ID.

Art Unit: 2131

84. Same rational for combination applies here as above in rejecting the claim 12.

85. As per claim 28, Tamiyuki teaches a method of locally wireless-connecting a plurality of terminal devices by using a set of a plurality of communication devices which can be freely inserted into and extracted from a slot of the terminal device to wireless-connect the terminal devices and which have a memory for storing a communication address of the own communication device, comprising the steps of:

a. allocating a communication device to each of the terminal devices to be wireless-connected (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101).

Tamiyuki does not teach into a slot of a specific terminal device, sequentially inserting communication devices allocated to other terminal devices to register communication addresses stored in the communication device at a transmission destination list table of said specific terminal device.

86. Vu teaches:

b. into a slot of a specific terminal device, sequentially inserting communication devices allocated to other terminal devices to register communication addresses stored in the communication device at a transmission destination list table of said specific terminal device (see similar rationale in rejecting the claim 20 (b) when each communication device is inserting to a specific terminal device which will be used as the concentrator or router to forward the address list table to the adjacent nodes in the same group).

Art Unit: 2131

c. inserting each communication device into a slot of an allocated terminal device, Tamiyuki as modified does not teach:

d. sequentially transmitting from said specific terminal device to other terminal devices, the contents of said transmission destination list table in which a communication address part of the current transmission destination communication device is replaced by the communication address stored in the communication device inserted into said specific terminal device, and each terminal device at the reception side, setting the contents of the received transmission destination list table at a transmission destination list table of the own device,

87. Aikawa teaches:

d. sequentially transmitting from said specific terminal device to other terminal devices, the contents of said transmission destination list table in which a communication address part of the current transmission destination communication device is replaced by the communication address stored in the communication device inserted into said specific terminal device, and each terminal device at the reception side, setting the contents of the received transmission destination list table at a transmission destination list table of the own device (Aikawa: see for example, Column 1 Line 53 – 57: This claim limitation (c) + (d) simply disclose that the specific terminal device forwards the Destination List Table to other peer device in the same group and the table contains all of the addresses of the devices within the group except the own address of the device that is going to use this table – i.e., the device that receives this forwarded Destination List Table does not need its own address).

Art Unit: 2131

88. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Aikawa within the system of Tamiyuki-Vu because Aikawa teaches static routing information for adjacent nodes can be set automatically without human intervention and flexibly.

e. transmitting and receiving data between the terminal devices into which the communication devices are inserted by using communication addresses of a transmission destination communication device and a transmission source communication device as a transmission destination address and a transmission source address. However, a person of ordinary skill in the art at the time the invention was made would realize the source and destination addresses are the mandatory header fields in the communication protocol.

89. As per claim 29, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 28). Vu further teaches said memory of each communication device, a common key inherent to the set is stored, said common key being for use in encryption of transmission data and decoding of reception data (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a common key in the symmetric key system).

90. Same rational for combination applies here as above in rejecting claim 28.

91. As per claims 31/32, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 28). Vu further teaches a part of the communication device partly projecting from the terminal device when inserted into the slot of the terminal device is assigned a number inherent to the communication device (see the same

Art Unit: 2131

rationale in rejecting the claim 12: The unique ID for authentication purpose is a number as well as an unique address).

92. Tamiyuki as modified does not teach the communication address of the communication device is composed of a high-order address part and a low-order address part in which part said number is set

93. However, a person of ordinary skill in the art at the time the invention was made would realize that the IP subnet address composes two parts where the high-order address part corresponds to the network address and the low-order address part corresponds to the specific Host ID.

94. Same rational for combination applies here as above in rejecting claim 28.

95. As per claim 33, Tamiyuki teaches a method of locally wireless-connecting a plurality of terminal devices by using a set of a plurality of communication devices which can be freely inserted into and extracted from a slot of the terminal device to wireless-connect the terminal devices and which have a memory for storing a communication address of the own communication device, comprising the steps of:

a. allocating a communication device to each of the terminal devices to be wireless-connected (Tamiyuki: see for example, Paragraph [0008] and Figure 1 Element 101).

Tamiyuki does not teach inserting each communication device into a slot of other terminal device than the allocated terminal device to register a communication address stored in the memory of the communication device at a transmission destination list table of the terminal device into which the communication device is inserted.

Art Unit: 2131

96. Vu teaches:

b. into a slot of a specific terminal device, sequentially inserting communication devices allotted to other terminal devices to register communication addresses and public keys stored in the communication devices at a transmission destination list table of said specific terminal device (see similar rationale in rejecting the claim 25 (b) when each communication device is inserting to a specific terminal device which will be used as the concentrator or router to forward the address list table to the adjacent nodes in the same group).

97. Vu further teaches said memory of each communication device, a secret key of the own communication device and a public key of other communication device of the same set are stored (Vu: see for example, Column 4 Line 57 – 60, Column 4 Line 62 – 64 and Column 7 Line 31 – 35: Vu discloses the cryptographic keys could be a private key in the public key cryptography system. However, a person of ordinary skill in the art at the time the invention was made would realize that the device only uses the public keys of other devices (not the private keys) to encrypt and transmit the data to the destination (i.e., other devices), which is inherited from the asymmetric cryptographic systems.

c. inserting each communication device into a slot of an allocated terminal device, Tamiyuki as modified does not teach:

d. sequentially transmitting from said specific terminal device to other terminal devices, the contents of said transmission destination list table in which parts of a communication address and a public key of the current transmission destination

Art Unit: 2131

communication device are replaced by the communication address and the public key stored in the communication device inserted into said specific terminal device and at the reception side terminal device, setting the contents of the received transmission destination list table at a transmission destination list table of the own device ,

Aikawa teaches:

d. sequentially transmitting from said specific terminal device to other terminal devices, the contents of said transmission destination list table in which parts of a communication address and a public key of the current transmission destination communication device are replaced by the communication address and the public key stored in the communication device inserted into said specific terminal device and at the reception side terminal device, setting the contents of the received transmission destination list table at a transmission destination list table of the own device (Aikawa: see for example, Column 1 Line 53 – 57: The claim limitation (c) + (d) simply disclose that the specific terminal device forwards the Destination List Table to other peer device in the same group and the table contains all of the addresses (and associated public keys) of the devices within the group except the own address (and public key) of the device that is going to use this table (i.e., the device that receives this forwarded Destination List Table does not need its own address and public key).

98. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Aikawa within the system of Tamiyuki-Vu because Aikawa teaches static routing information for adjacent nodes can be set automatically without human intervention and flexibly. The routing information herein

Art Unit: 2131

includes not only the communication address but also the public key to enable the data transmission (for security encryption purpose).

e. transmitting and receiving data between the terminal devices into which the communication devices are inserted by using communication addresses of a transmission destination communication device and a transmission source communication device as a transmission destination address and a transmission source address, using a public key of the transmission destination communication device for encrypting transmission data and using a secret key for decoding reception data. It would be obvious to a person of ordinary skill in the art at the time the invention was made to realize this basic network setup practice before the operation because (1) the source and destination addresses are the mandatory header fields in the communication protocol, and (2) the device only uses the public keys of other devices (not the private keys) to encrypt and transmit the data to the destination (i.e., other devices), which is inherited from the asymmetric cryptographic systems.

99. As per claim 34, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 33). Vu further teaches a part of the communication device partly projecting from the terminal device when inserted into the slot of the terminal device is assigned a number inherent to the communication device (see the same rationale in rejecting the claim 12: The unique ID for authentication purpose is a number as well as an unique address).

Art Unit: 2131

100. Tamiyuki as modified does not teach the communication address of the communication device is composed of a high-order address part and a low-order address part in which part said number is set.

101. However, a person of ordinary skill in the art at the time the invention was made would realize that the IP subnet address composes two parts where the high-order address part corresponds to the network address and the low-order address part corresponds to the specific Host ID.

102. Same rational for combination applies here as above in rejecting claim 33.

103. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu, in view of Aikawa (Patent Number: 5884047), hereinafter referred to as Aikawa, and in view of de la Koenck (Patent Number: 6006100), hereinafter referred to as de la Koenck.

104. As per claim 30, Tamiyuki-Vu-Aikawa teaches the claimed invention as described above (see claim 28). Tamiyuki as modified does not teach into one slot of a relay device having a plurality of slots and having a function of relaying data between slots, a communication device of a first set is inserted and into other one slot, a communication device of a second set is inserted to enable communication between a terminal device into which other communication device of the first set is inserted and a terminal device

Art Unit: 2131

into which other communication device of the second set is inserted through said relay device.

105. Koenck teaches a relay device uses dual transceivers to relay data messages between two different networks or group of devices (Koenck: see for example, Column 4 Line 53 – 57).

106. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Koenck within the system of Tamiyuki-Vu-Aikawa because Koenck discloses a structure to relay two disjoint communication groups of devices in the physical layer.

107. Same rationale of combination applies here as above in rejecting the claim 28.

108. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tamiyuki (Publication Number: 07-327089), hereinafter referred to as Tamiyuki, in view of Vu (Patent Number: US 6557104 B2), hereinafter referred to as Vu, in view of Billstrom (Patent Number: 5729537), hereinafter referred to as Billstrom, and in view of de la Huerga (Patent Number: 5960085), hereinafter referred to as de la Huerga.

109. As per claim 10, Tamiyuki-Vu-Billstrom teaches the claimed invention as described above (see claim 9). Tamiyuki as modified does not teach when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted.

110. de la Huerga teaches when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted (de la Huerga: see for example, Column 4 Line 40 – 67 and Column 5 Line 1 – 11: de la Huerga teaches a security system equipped with a wireless device to exchange authentication information with the security badge of a system user (de la Huerga: see for example, Column 4 Line 42 – 43). After the authentication and system in service, the computer terminal continues to monitor the signal path between the security badge and the computer terminal. If the system user turns away from the computer terminal, then the keyboard is locked and the screen is blanked off (de la Huerga: see for example, Column 5 Line 3 – 5).

111. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of de la Huerga within the system of Tamiyuki-Vu because de la Huerga teaches a limited access system for restricting and monitoring between smart devices.

112. As per claim 11, Tamiyuki-Vu-Billstrom teaches the claimed invention as described above (see claim 9). Tamiyuki as modified does not teach when the communication device is extracted from the slot after authentication between the terminal device and the communication device is obtained, bringing the terminal device to a locked state where none of input by a user is accepted.

113. de la Huerga teaches when the communication device is extracted from the slot after authentication between the terminal device and the communication device is

Art Unit: 2131

obtained, bringing the terminal device to a locked state where none of input by a user is accepted (de la Hueraga: see for example, Column 4 Line 40 – 67 and Column 5 Line 1 – 11).

114. Tamiyuki as modified does not teach when the communication device is inserted into the slot of the locked terminal device to obtain authentication between the terminal device and the communication device, releasing the terminal device from the locked state.

115. de la Hueraga teach when the communication device is inserted into the slot of the locked terminal device to obtain authentication between the terminal device and the communication device, releasing the terminal device from the locked state (de la Hueraga: see for example, Column 4 Line 40 – 67 and Column 5 Line 10 – 11: de la Hueraga teaches if the security badge is not properly positioned for more than a preset period of time, the system user will be logged off automatically. This implies the system user needs to go through the authentication process again after returning back to the proper position).

116. Same rational for combination applies here as above in rejecting the claim 10.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

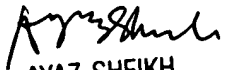
Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100